AASG
Accountancy AML Supervisors' Group

Alternative Banking Platforms (ABPs) Money Laundering and Tax Fraud

Extract from NCA Amber ALERT of November 2023 (Reference 0734-NECC)

Overview

This Alert describes money laundering and tax fraud typologies using 'Underground Banking' involving both nonbank FinTechs who are corrupt and complicit in criminal activity and provide money laundering as a service to criminals (as part of international money laundering networks), or firms who are unwitting and/or negligent who have weak AML controls. The feature of the activity in this report involves the use of facilities provided by nonbank FinTechs; these firms are payment service providers that provide digital banking, international payments and forex services and may provide domestic payments or issue e-money.

Executive Summary

Underground Banking is an informal way of providing financial services. It includes community-based financial schemes and informal value transfer systems (IVTS) such as Hawala and Other Similar Service Providers ("HOSSPs"). It is largely a secretive financial ecosystem that runs parallel to and shadows the existing recognised UK and global financial systems. The community in this context may be based on cultural, religious, ethnic (such as diaspora communities in the UK), and/or social / familial lines as well as the criminal community.

Those engaged in underground banking frequently use services provided by banks, Non-Bank Payment Service Providers (NBPSPs), and other professionals to facilitate the movement of funds.

This report focuses on underground banking activity including domestic and global payments, and informal loan schemes involving nonbank ABPs[1]. These payments normally connect globally with the formal banking and payments system and most payment orders are executed as bank-to-bank payments. The exception to this is when payment orders are executed within closed systems such as the mobile money ecosystem or covert criminal schemes using Highly Secured Devices (HSDs) such as EncroChat and the SkyECC tool or social media Apps such as WhatsApp and WeChat. All these services use End-to-End Encryption which is a method to secure communication that prevents third parties from accessing data while it is transferred from one end system or device to another. The data is encrypted on the sender's system/device and only the intended recipient can decrypt it. The red flags in this report are known indicators previously associated with money laundering and tax fraud typologies, such as the use of cash, the exploitation of payment services sector and manipulation of VAT repayment schemes.

The following JMLIT+ Alerts provide more details on risk and thematics relevant to some of the activity described in this report (available in previously distributed summary alerts or contact your professional body for more details):

- 0624-NECC Daigou money laundering and tax crime typologies May 2021;
- 0678-NECC money laundering and tax fraud typologies involving unregistered MSBs March 2022;
- 0701-NECC Fraud and Money Mules, 0702-NECC Fraud Cashing-Out Mechanisms August 2022;
- 0709-NECC Money Laundering and Tax Fraud Typologies: 'cuckoo smurfing' December 2022;
- 0710-NECC Illicit Finance Risks Associated with NETPs as cross-border e-commerce traders December 2022.

[1] An ABP is the collective term used by HMRC for nonbank FinTechs; digitally enabled systems that offer financial services without a traditional banking license

Key takeaways and potential Red Flag Indicators from case studies

- Use of shell companies (with no PAYE employees and a virtual/managed office as the registered office) to gain access to UK bank accounts. Virtual IBANs (v-IBANs) issued by the UK clearing bank to the shell company (on this occasion an authorized Electronic Money Institution (EMI)) that were anonymously sublet to Organised Crime Groups (OCGs), creating anonymous accounts and covert access to the UK banking system and UK and offshore cryptoasset exchanges.

- Cash deposited in non-personal accounts through Post Office everyday banking facilities and immediately transferred to a Cryptoasset business, which exchanged it into Cryptoassets.

- Cash deposited in mule accounts (some non-personal accounts but mainly student accounts) through the Post Office everyday banking facilities and funds immediately dispersed to load pre-paid cards issued by EMIs.

- Tax reliefs, typically, VAT repayments received from HMRC, paid into accounts that are not commensurate with account turnover. For example, £1.2 million declared sales, (monthly or quarterly VAT period) by a criminal Daigou, may result in a £200,000 VAT repayment being made by HMRC (one-sixth of the sales value). Although typically, the £1.2 million sales income is not paid into the account by the overseas customer during the period.

- Exploitation of UK correspondent banking services to UK FinTech, which in turn provide banking services to overseas online gambling platforms. Pre-paid cards loaded with cash are then used to upload funds to online gambling wallets, which in turn are used to credit personal bank accounts (under the guise of winnings).

- Merchant Acquirers accepted and enabled MobilePay payments from Chinese digital wallets (such as AliPay and WeChat Pay) or China UnionPay accounts for purchases at UK retailers.

Electronic transactions are more traceable than cash-based remittances. And whilst some high street retail payment firms use FinTech solutions to provide payments, a key feature of the nonbank FinTechs is that most commercial retail payment firms offering services to consumers and corporates do not tend to operate counters, instead offering services remotely through on-line portals and Apps, and providing banking as a service to customers who enter into a business relationship rather than simply offering *ad hoc* and walk-up on-demand payment services. This enables a customer's transaction history to be monitored against their customer profile and reduces risk compared to firms that offer ad hoc and execute one-off payment transactions for customers.

If you have clients engaged in the activity outlined above and want to read further details, then full case studies can be read in the original JMLIT alert sent with this one.

Risk Matrix - Potential high-risk nonbank FinTech business models

The following are potential indicators of high-risk nonbank FinTech activity that may give cause for concern. These indicators should be considered cumulatively as grounds for further enquiry and escalation.

The expression "high-risk jurisdictions" below means jurisdictions on the FATF grey-list, the UK Sanctions List, or "those jurisdictions assessed to be particularly relevant to the cross-border money laundering risks faced and posed by the UK[2]" cited in the National Risk Assessment (NRA); which are China, Hong Kong, Pakistan, Russia, United Arab Emirates (UAE), and UK Crown Dependencies and Overseas Territories.

Assessed Factor	Potential high-risk nonbank FinTech business models/activity
1. Corporate Entity	
	• Firms with complex ownership structures including offshore ownership. • UK firms whose directors / owners who are domiciled in high-risk jurisdictions.

[2] Paragraph 4.15 of the UK National risk assessment of money laundering and terrorist financing 2020 https://assets.publishing.service.gov.uk/government/NRA_2020_v1.2.pdf

- Off-shore entities providing services for UK entities and/or onboarding UK customers.

- Inexperienced BOOMs[3] sometimes with no financial sector experience. To circumvent this red flag, some firms will use 'rent-a-SIF' (Significant Influence Function), although there aren't actually Senior Management Functions SIFs or SMFs in payments firms, the same general idea certainly applies, though; temporary employment of a person (in a SIF or SMF) to give the impression that the firm has competent management. Typically, such persons may then resign once an application is authorised by the FCA.

- Change of ownership/directors/SMFs. OCGs / organised crime networks (OCNs[4]) sometimes infiltrate the financial sector by purchasing or investing in an existing payment firm. This is frequently achieved by using 'clean skin(s)' to act as BOOMs. The Transparency International UK report ***Together in Electric Schemes***[5] published March 2022 stated, "Using open-source analysis we found EMI licences and accounts for sale to buyers around the world, including:

    - *38 Russian and Ukrainian language corporate services websites that are selling British EMI accounts alongside secretive offshore companies for clients who want to hide their identities.*

    - *Licenced UK EMIs advertised for sale on LinkedIn and corporate service websites, with prices ranging from £600,000 to £1.5 million."*

Nonbank FinTechs who use virtual/serviced office addresses. Typically, in Central London to give the impression of a London presence (most nonbank FinTechs are based in Central London).

2. Jurisdictions

- Firms operating in high-risk remittance corridors. This includes high-risk jurisdictions.

- 'Regulatory Arbitrage' may involve UK high-risk customers (individuals or companies) being onboarded by and using services of banks and nonbank FinTechs in high-risk jurisdictions who have weaker AML/CFT controls than the UK. For example, de-risking of the remittance market has meant that most high street retail money transmitters in the UK do not enjoy UK banking facilities and many now bank offshore, frequently in high-risk jurisdictions.

Commercial retail nonbank FinTechs in the UK can be differentiated from high street retail money transmitters because they tend to enjoy UK banking facilities. Some of these firms still use services offered by offshore firms. For example, under passporting arrangements that shall remain in force in the UK until December 2023.

3.1 Customers

- Customers who are owners/directors (i.e. 'owner-managers' typically sole-directors/100 percent shareholders) of more than one corporate entity in different trade sectors requesting to use the FinTech's services.

- New companies; i.e. the corporate entity may be less than 22 or 24 months old and not yet filed accounts at Companies House.

- Off-shore customers who are domiciled in high-risk jurisdictions.

- Customers who use virtual/serviced office addresses or residential addresses as their PPOB.

3.2 Customers – Cross-border traders

- Customers who purport to engage in cross-border trade that do not have an EORI.

[3] BOOM's are Beneficial Owner, "officer" or Manager of a relevant person where they are PSPs, (reg 58(1)
[4] An OCN, is a network of criminals and/or OCGs that collaborate to commit crime.
[5] Together in Electric Schemes - Transparency International UK

- Businesses may need an Economic Operators Registration and Identification number (EORI number) to move goods: between Great Britain (England, Scotland and Wales) or the Isle of Man and any other country (including the EU)

    - between Great Britain and Northern Ireland or the Channel Islands
    - between Northern Ireland and countries outside the EU

Check an EORI number. Check a business's EORI number, used to import and export goods from the UK.

4.1 Products / Services – Virtual accounts

There is no requirement to 'know your customers customer' (KYCC). This enables corrupt FinTech's to offer criminal clients anonymous accounts without the knowledge on the bank acting as its IPSP who processes payments on behalf of their nonbank FinTech client

4.2 Products / Services – Prepaid cards

- UK companies used by criminal Daigou principals to engage in money laundering and tax fraud frequently use account facilities and services provided by nonbank FinTechs

- HMRC observes that whilst most criminal Daigou use AMEX card facilities[6], several also use pre-paid card facilities provided by nonbank FinTechs. The main use is for domestic purchases at merchants POS activity and on-line. Criminal Daigou principals frequently obtain hundreds of cards so that they can be distributed amongst their network of hundreds of Daigou shoppers. We are aware than whilst KYC is conducted on the principal customer, the card issuer (normally an EMI) may not conduct any additional KYC on the named card holder. This means that any name (natural or legal) may be printed on the prepaid card. Several hundred prepaid cards may be issued in the names of third parties (individuals or other companies) who are not employed by or connected to the company. The retailer accepting the payment on the prepaid card may assume that the identity of the user has been verified (which is what is expected to happen with a bank card), whereas the user' s identity has not normally been checked at all. Risks exist where no CDD is conducted on these additional cards.

- Criminal Daigou principals frequently trade with high-risk jurisdictions including China and Hong Kong. Trading with Macau, South Korea, Vietnam and elsewhere is also common.

Prepaid cards used by third parties to purchase goods above the £85,000 VAT threshold when that individual is not registered with HMRC for VAT. Check a UK VAT number. Use this service to ***check*** if a UK ***VAT registration*** number is valid and the name and address of the business the number is ***registered*** to.

4.3 Products / Services - MobilePay

- Chinese registered Mobile phones used to access Alipay / WeChat pay wallets to evade Chinese Foreign Exchange Controls. Frequently payments exceed the $10,000 USD per person daily limit and/or $50,000 USD per person annual limit.

- Daigou principals control Daigou shoppers who use Chinese registered mobile phones to access Chinese money held in nonbank FinTech accounts (Alipay/WeChat). Multiple accounts/wallets may be used in a single transaction in order to ensure that each single transaction is below the $10,000 USD daily limit for each account.

Registered payment firms processing payments for unregulated operators whose customers are purporting to be cross-border e-commerce businesses using Alipay / WeChat services. These services are only available to Chinese residents and commercial payments are not expected to be made using these social media-based payment platforms aimed at Chinese consumers.

[6] Key reasons included the ability of the Card holder to request AMEX to issue up to 99 supplementary cards and pay balances using third-party cash payments using Giro Slips through a Head Office Collection Account (HOCA) facility. The number of supplementary cards that can be issued has been reduced to 5 https://www.americanexpress.com/uk/benefits/supplementary-cards/ and the HOCA facility has now been withdrawn https://www.americanexpress.com/uk/customer-service/how-to-make-payment.html.

4.4. Products / Services – Merchant Acquirer / Mobile Point-of-Sale (Chip 'n' Pin) devices
• High street retail MSBs are frequently co-located with retail businesses. Complicit and corrupt firms frequently use genuine ID documents obtained from associated businesses to 'cover' criminal transactions. For example, Travel agents. • High street retail MSBs using Merchant Acquirer Chip 'n' Pin devices in a manner not commensurate with normal trade. For example, migrant remittances/consumer remittances frequently exceeding £350 average per transaction. The average "send" transaction value for each outbound remittance was USD 426.70 (334.19 GBP), in 2020 for a global brand name payment firm in 2020. • Volume / Value / Velocity of transactions on the device is not commensurate with normal trade. For example, multiple high-value transactions (i.e. above £1,000) within minutes of each other. The IP address of the Merchant Acquirer Chip 'n' Pin devices being used doesn't match the businesses PPOB.
5 Transactions – Inability to detect linked transactions
A nonbank FinTech firm aggregated payments up from multiple agents and sub-processors. The information they have on the underlying individuals (originators of the payments) is hugely fragmented. In some instances, they only obtained the payers name. Sometimes the name was verified with an ID. On occasions, the only information on the payer they received was a mobile number. Under these circumstances, it would be impossible for them to tell if the same individual was using their services at 20 different branches because there was no way to detect linked transactions. They were processing transactions to high-risk jurisdictions but seemingly had no concept of the SCHEDULE 3ZA High-Risk Third Countries list. Their high-risk list was solely based on OFAC sanctions. When onboarding a customer, it is imperative that appropriate CDD is conducted. This involves verifying the customers ID when necessary. For example, for all cash-based transactions and transactions exceeding 1,000 EUR or equivalent in any currency. It is unlawful to execute a payment order unless appropriate CDD is conducted Requirement to cease transactions etc. Poor data collection and storage methods (relevant information on customers' needs to be searchable to enable linked transactions to be identified) will lead to poor outcomes because the data cannot be properly analysed and used. Some firms still rely on Excel spreadsheets to store relevant information. This is not an effective way to manage information and may lead to the risk of failing to appropriately identify and verify a person's identity engaged in linked transactions etc.

Case Studies

The following case studies are drawn from examples experienced by JMLIT members, HMRC and compliance experts involved in the project identifying and investigating examples of suspected financial crime involving the use of FinTech and Forex payment firms. They are intended to provide insight into recent examples of money laundering and / or tax fraud activity where the criminal or criminal group used the services of a nonbank FinTech and Forex payment firm. The case studies include examples of both unwitting, negligent and/or complicit / corrupt FinTech and Forex payment firm's activity.

Where you consider these case studies may be relevant to your firm, detailed case studies are available within the full published JMLIT alert.

Case Study	Summary
Corrupt FinTech providing anonymous virtual accounts and 'nested' services	UK law enforcement partners discovered that an Authorised EMI was complicit in laundering the proceeds from mainly MTIC VAT Supply Chain Fraud (MTIC VSCF36), Boiler Room frauds37 and some drug trafficking proceeds.
Use of MobilePay to engage in ML and Tax Fraud using criminal Daigou.	In one case £400,000 of premium watches were purchased in one month using Renminbi held in Alipay wallets. The alleged criminal Daigou purchased more than £2 million of luxury watches, and more than 80 percent were purchased using MobilePay; Renminbi accessed via Chinese-registered mobile phones (Alipay funds) at UK retailers EPOS.

Use of Pre-Paid cards provided by an EMI in criminal Daigou activity.	Several criminal Daigou operators used pre-paid cards issued by EMIs to purchase luxury goods funded by street cash. Millions in street cash is used to load pre-paid cards structured through UK Mule Accounts to criminal Daigou companies who immediately disperse funds to load pre-paid cards issued by EMIs.
Criminal Hawala IVTS settlement by unwitting FinTechs	HMRC are investigating several unregistered HOSSPs engaged in illegal money remittance activity. Typically, migrant remittances for local communities where low value payments, typically under £350, are made.
Laundering street cash through pre-paid cards	A bank held a correspondent banking relationship with a UK FinTech, who provided banking services to an online gambling company registered and regulated in Malta.
Corrupt MSBs using Merchant Acquiring payment services to laundering the proceeds of Social engineering and cyber fraud	An Investigation by the Metropolitan Police Service (MPS), HMRC and banks identified a money laundering Organised Crime Network (OCN) based in London who have obtained bank accounts in the names of individuals (with or without their knowledge) or have incorporated UK companies that the OCN obtains bank accounts for.
Use of nonbank FinTechs to commit MTIC VAT Supply Chain Fraud	An ABP ("MSB") identified a network of recently incorporated companies purporting to be involved in wholesale of household fast-moving-consumer goods; food and drinks from major brands such as Coca Cola, Red Bull, Nestle and Mars. The companies FX requirement was to sell GBP and send EUR to a purported supplier in the Eurozone. One UK wholesaler incorporated for less than two years filing micro-company accounts turned over more than £7 million per year. Funds were usually received in rounded numbers and the entire balance was dispersed immediately in quick succession. Initially, accounts did not appear to be connected.

Suspicious Activity Reporting [SARs]

If you know or suspect that there has been money laundering or terrorist financing activity (including as a result of information provided to you by the NCA) and your business falls within the regulated sector, then you are reminded of the obligations to make reports to the NCA under Part 7 Proceeds of Crime Act 2002 and the Terrorism Act 2000. If you decide to make a report in this way you should adopt the usual mechanism for doing so, and it will help our analysis if you would include the reference **0734-NECC** within the text. This reference is specific to the Alerts process; where appropriate, we would ask that this is used in addition to the ongoing use of the Glossary of Terms. Guidance on making suspicious activity reports is available at www.nationalcrimeagency.gov.uk.

Data Protection Considerations

Please consider your obligations under the relevant data protection regulations and where necessary remove any related personal data from your systems securely and within a satisfactory timeframe.

Disclaimer

The Accountancy AML Supervisors' Group (AASG) accepts no responsibility for any loss, damage or expense arising in connection with the use of information in this alert. Any use will be taken to signify agreement to these conditions.